The following message from the Director of NSA is for your information.
No specific actions required at this time.

Tom
Thomas J. Aubin
Information Systems Security Program Manager
United States Army Corps of Engineers

-----Original Message-----
From: Loranger, Phillip J., Mr., DISC4 [SMTP:LoranPJ@hqda.army.mil]
Sent: Friday, June 04, 1999 9:28 AM
To: DISC4 IAO
Subject: NSIRC ADVISORY - IMPROVING WEB SITE SECURITY

M DIRNSA FT GEORGE G MEADE MD//NSIRC/X7/SIPO//

TO SECDEF WASHINGTON DC//C3I/IA//
HQ AFCIC WASHINGTON DC//SY/SYN//
DA WASHINGTON DC//SAIS/SAIS-ZB/SAIS-PAC-I//
DEPT OF COMMERCE WASHINGTON DC//OIPR//
CIA WASHINGTON DC//CTG/DI/OTI/IWT//
DIA WASHINGTON DC//DS/SY/TWI/J2J/DAJ2A//
DEPT OF ENERGY WASHINGTON DC//CIAC/HR43/HR44//
RUCNFB/FBI WASHINGTON DC//NIPC/NSD(NS-6)//
FEMA HQ WASHINGTON DC//JJJ//
GSA OFFICE INFO SECURITY WASHINGTON DC//TI/FTS//
JOINT STAFF WASHINGTON DC//J6//
DEPT OF JUSTICE WASHINGTON DC//ISPG/CSS/IMSS//
CMC WASHINGTON DC//CS/C4I//
CNO WASHINGTON DC//N6/N64//
NCS WASHINGTON DC//JJJ/IA/NCC//
WHITE HOUSE NATIONAL SECURITY COUNCIL WASHINGTON DC//JJJ//
WHITE HOUSE OMB WASHINGTON DC//JJJ//
RUEHC/DEPT OF STATE WASHINGTON DC//DS/CIS/IST/ACD/IRM/OPS/ITI/SI//
DEPT OF TREASURY WASHINGTON DC//SEN//
HQ DISA WASHINGTON DC//D25/D331/D333/D3332//
DEPT OF EDUCATION WASHINGTON DC//JJJ//
FCC WASHINGTON DC//JJJ//
NASA WASHINGTON DC//JL//
NIMA RESTON VA//JJJ//
NRC WASHINGTON DC//T6E46/O2D15//
NRO WASHINGTON DC//CIO/WF3/COMM350/IROC//
JTF-CND WASHINGTON DC//J2/J3//

DEPT OF TRANSPORTATION WASHINGTON DC

UNCLAS
NSIRC-ADV-0024-99

SUBJECT: NSIRC ADVISORY - IMPROVING WEB SITE SECURITY

1. IN LIGHT OF RECENT HACKING ACTIVITIES DIRECTED AGAINST U.S. GOVERNMENT WEB SITES, THE FOLLOWING GENERAL GUIDANCE CONCERNING NETWORK SYSTEMS SECURITY IS OFFERED:
A) CREATE A SYSTEM SECURITY POLICY THAT PROVIDES GUIDELINES FOR CONFIGURING SYSTEMS.
B) REMOVE/TURN-OFF ALL NONESSENTIAL SERVICES (E.G. TELNET, FTP, E-MAIL, ETC.). MANY OF THESE SERVICES HAVE SECURITY WEAKNESSES OF THEIR OWN AND UNNECESSARILY INCREASE THE LIKELIHOOD A SYSTEM VULNERABILITY. CONSIDER STRENGTHENING THE OPERATING SYSTEM KERNEL BY REMOVING CODE FOR UNNECESSARY SERVICES THEN RECOMPILING THE KERNAL.
IF POSSIBLE, MAINTAIN THE WEBSERVER MACHINE AS PURELY A WEBSERVER WITH NO OTHER SERVICES ENABLED EXCEPT DNS.
C) STANDARDIZE ON ONE VENDOR PLATFORM - E.G. ALL SUNS OR SGI'S RUNNING THE SAME OPERATING SYSTEM.
D) UPDATE OPERATING SYSTEMS TO THE CURRENT RELEASE AND/OR ENSURE THE LATEST PATCHES FOR THE RELEASE USED ARE INSTALLED.
E) CONSIDER THE USE OF FIREWALLS AND OR FILTERING ROUTERS IN YOUR LAN ARCHITECTURE IN FRONT OF THE WEB-SERVER TO PROVIDE ADDED LAYERS OF SECURITY/SEPARATION FROM THE NETWORK.
F) REMOVE CGI-SCRIPTS NOT BEING USED FROM THE SERVER. SOME CGI-SCRIPTS HAVE SERIOUS SECURITY VULNERABILITIES.
G) USE SECRUITY TOOLS JUDICIOUSLY - THIS SHOULD ALWAYS BE DONE CAREFULLY AS THESE TOOLS WILL BE CREATING FILES THAT DOCUMENT NETWORK VULNERABILITIES. TOOLS SHOULD BE USED CAREFULLY AS IT IS POSSIBLE TO CRASH A NETWORK IF USED IMPROPERLY. TOOLS SHOULD ALSO BE USED IN CONSULTATION WITH AN ORGANIZATION'S SECURITY POLICY AND GENERAL COUNSEL.
H) INSPECT YOU LOGS ROUTINELY. BOTH WEB SERVERS AND OPERATING SYSTEMS HAVE THE CAPABILITY TO LOG CRITICAL EVENTS THAT WILL AID IN DISCOVERY AND RECONSTRUCTION OF A PENETRATION ATTEMPT.
I) DO NOT RUN THE WEB SERVER WITH ROOT OR ADMIN PRIVILEDGES. OLDER WEB SERVERS SOFTWARE MAY ALLOW PRIVILEDGED ACCESS WHICH OPENS POSSIBLITIES TO KNOWN ATTACKS (I.E. CGI-BIN, PHF). UPGRADE WEBSERVER SOFTWARE WHEN POSSIBLE.
J) IF THE INFORMATION ON THE WEBSERVER IS STATIC OR UPDATED

INFREQUENTLY, CONSIDER RUNNING THE WEB SERVER FILE SYSTEM AS READ ONLY.

2. ORGANIZATIONAL SECURITY POLICY SHOULD CONSIDER NETWORK SECURITY PLANNING, SITE SECURITY POLICY, AND RISK ANALYSIS. RESULTS OF A RISK ANALYSIS SHOULD PROVIDE ASSISTANCE WHEN DETERMINING INFORMATION TO BE PROTECTED, FROM INFORMATION AVAILABLE TO THE PUBLIC. TO THE GREATEST EXTENT POSSIBLE GOVERNMENT WEB SERVERS SHOULD BE SEGREGATED FROM INTERNAL NETWORKS TO REDUCE EXTENT OF DAMAGE FROM UNAUTHORIZED USERS. THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) HAS ABUNDANT INFORMATION ON DEVELOPING SECURITY POLICY ON ITS WEB SITE (WWW.NIST.GOV/PUBLICATIONS).

3. MANY VULNERABILITIES EXIST IN COMMERCIAL COMPUTER OPERATING SYSTEMS AND WEB SERVER APPLICATIONS. SYSTEM ADMINISTRATORS SHOULD CONDUCT INITIAL AND PERIODIC SURVEYS OF VULNERABILITIES TO DETERMINE CORRECTIVE MEASURES AND UPDATED SECURITY PATCHES THAT SHOULD BE APPLIED TO THEIR SITES. GUIDANCE MAY BE FOUND AT THE CARNEGIE MELLON CERT WEB SITE (WWW.CERT.ORG).

4. A NUMBER OF EFFECTIVE WORKING AIDS EXIST FOR THE SYSTEM ADMINISTRATOR TO DETERMINE SYSTEM VULNERABILITIES, AND THESE AIDS ARE INVALUABLE TOOLS FOR USE IN ASSESSING A SYSTEM, AS WELL AS ASSISTING IN THE DAY-TO-DAY SECURITY MANAGEMENT OF WEB SITES. ADDITIONAL INFORMATION REGARDING WORKING AIDS MAY BE FOUND AT THE FEDCIRC WEB SITE (WWW.FEDCIRC.GOV).

5. THE NATIONAL SECURITY AGENCY OFFERS A NUMBER OF SYSTEM ASSESSMENT SERVICES WHICH MAY BE OF USE TO YOUR DEPARTMENT OR AGENCY. FOR MORE INFORMATION ON THESE SERVICES PLEASE CALL (CIVIL AGENCIES) 410-854-5790 OR (MILITARY DEPARTMENTS) 410-854-4391. IF YOU HAVE QUESTIONS REGARDING THE NATIONAL SECURITY INCIDENT RESPONSE CENTER OR THIS ADVISORY PLEASE CONTACT THE NSIRC STAFF ON 410-854-7070.

BT
NNNN